Frobenius' result on simple groups of order $\frac{p^3-p}{2}$

Paul Monsky

Brandeis University, Waltham MA 02454-9110, USA
monsky@brandeis.edu

Abstract

The complete list of pairs of non-isomorphic finite simple groups having the same order is well-known. In particular for $p > 3$, $PSL_2(\mathbb{Z}/p)$ is the "only" simple group of order $\frac{p^3-p}{2}$. It's less well-known that Frobenius proved this uniqueness result in 1902. This note presents a version of Frobenius' argument that might be used in an undergraduate honors algebra course. It also includes a short modern proof, aimed at the same audience, of the much earlier result that $PSL_2(\mathbb{Z}/p)$ is simple for $p > 3$; a result stated by Galois in 1832.

1 Background

Let p be a prime and $SL_2(\mathbb{Z}/p)$ be the group of 2 by 2 determinant 1 matrices with entries in $\mathbb{Z}/p$. The quotient, $PSL_2(\mathbb{Z}/p)$, of $SL_2(\mathbb{Z}/p)$ by $\{\pm\mathbf{I}\}$ is for $p > 2$ a group of order $\frac{p^3-p}{2}$. Galois [2] introduced and studied this group; in his 1832 letter to Auguste Chevalier he says that it is easily shown to be simple for $p > 3$. (There are many proofs of simplicity. I'll give a short one in section 6.) In 1902 Frobenius [1] classified certain transitive permutation groups on $p+1$ letters up to permutation isomorphism, and deduced as a corollary that $PSL_2(\mathbb{Z}/p)$ is the "only" simple group of order $\frac{p^3-p}{2}$.

Frobenius' proof of this very early result in the classification of the finite simple groups, though elementary, isn't well-known and hasn't found its way into textbooks. In this note I give a version of it, based on Sylow theory and the cyclicity of $(\mathbb{Z}/p)^*$. This version could perhaps be presented in an undergraduate honors algebra course. I thank Jim Humphreys for his close reading of this note, his encouragement, and his expository suggestions.

Another description of $PSL_2(\mathbb{Z}/p)$ will be useful. Let V be the space of column vectors, $\binom{x}{y}$, with entries in $\mathbb{Z}/p$. $SL_2(\mathbb{Z}/p)$ acts on the set consisting of the

$p+1$ one-dimensional subspaces of V. We identify this space with $\mathbb{Z}/p \cup \{\infty\}$ as follows. Given a subspace with generator $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, map it to the element $z = \frac{x}{y}$ of $\mathbb{Z}/p \cup \{\infty\}$. Since $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ is mapped to $\left(\begin{smallmatrix} x+y \\ y \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and to $\left(\begin{smallmatrix} -y \\ x \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, the images of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ are the translation $z \to z+1$, and the involution $z \to -\frac{1}{z}$. Easy arguments with row and column operations show that $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ generate $SL_2(\mathbb{Z}/p)$. Since the kernel of the action of $SL_2(\mathbb{Z}/p)$ consists of $\mathbf{I}$ and $-\mathbf{I}$, $PSL_2(\mathbb{Z}/p)$ identifies with the transitive group of permutations of $\mathbb{Z}/p \cup \{\infty\}$ generated by $z \to z+1$ and $z \to -\frac{1}{z}$.

I'll prove the following (version of a) result of Frobenius, and its easy corollary:

Classification Theorem. Let $p \neq 2$ be prime and G be a transitive group of permutations of $\mathbb{Z}/p \cup \{\infty\}$. Suppose $|G| = \frac{p^3-p}{2}$, and that G contains the translations. Then one of the following holds:

(a) $z \to -\frac{1}{z}$ is in G. (In this case the description of $PSL_2(\mathbb{Z}/p)$ given above and the fact that $|G| = |PSL_2(\mathbb{Z}/p)|$ tell us that G is generated by $z \to z+1$ and $z \to -\frac{1}{z}$, and is permutation-isomorphic to $PSL_2(\mathbb{Z}/p)$ in its action on the 1-dimensional subspaces of V.)

(b) $p = 7$ and G contains the involution $(0\infty)(13)(26)(45)$ or the involution $(0\infty)(15)(23)(46)$. In these cases G is generated by $z \to z+1$, $z \to 2z$, and the involution, and has a normal subgroup of order 8.

Corollary. When $p > 3$, $PSL_2(\mathbb{Z}/p)$ is, up to isomorphism, the only simple group of order $\frac{p^3-p}{2}$.

The theorem is trivial when $p = 3$. For now $|G| = 12$ and G is a permutation group on 4 elements. So G consists of the even permutations, and thus contains $(0\infty)(12)$. In the following sections we prove the theorem for $p > 3$, but now we show how the corollary follows. Suppose G is a simple group of order $\frac{p^3-p}{2}$ with $p > 3$. Then p divides $|G|$ and G has $mp+1$ p-Sylow subgroups; since G is simple $m > 0$. Furthermore $\frac{p^2-1}{mp+1}$ is an integer $\equiv -1$ (p) and so is $\geq p-1$; it follows that $m = 1$. G acts on the set S consisting of the $p+1$ p-Sylows, and by Sylow theory the action is transitive. Since G is simple, the action is faithful. Select an element σ of G of order p. This element acts by a p-cycle on S; denote the element it fixes by ∞. We may label the remaining elements of S with tags in $\mathbb{Z}/p$ so that σ is the translation $(01 \cdots p-1)$, $z \to z+1$, of $\mathbb{Z}/p \cup \{\infty\}$. If we view G as a group of permutations of $\mathbb{Z}/p \cup \{\infty\}$, the hypotheses of the classification theorem are satisfied. Since G has no normal subgroup of order 8, we're in the situation of (a), and we conclude that G is isomorphic to $PSL_2(\mathbb{Z}/p)$.

2 Easy facts about G

For the rest of this note G is a group satisfying the hypotheses of the classification theorem. Then the stabilizer, G_∞, of ∞ in G contains the translations and so is transitive on $\mathbb{Z}/p$. Consequently:

Lemma 2.1. *G is doubly transitive on $\mathbb{Z}/p \cup \{\infty\}$.*

Definition 2.2. *K is the subgroup of G consisting of elements fixing 0 and ∞. $\bar{K}$ consists of the elements of G interchanging 0 and ∞. $H = K \cup \bar{K}$ is the stabilizer of $\{0, \infty\}$ in G.*

Since G is doubly transitive, $|K| = \frac{|G|}{p(p+1)} = \frac{p-1}{2}$. Double transitivity also shows that $\bar{K}$ is non-empty. So K is of index 2 in H, and $|\bar{K}| = |K| = \frac{p-1}{2}$.

Definition 2.3. *R is the set of squares in $(\mathbb{Z}/p)^*$, N the set of non-squares.*

Since $(\mathbb{Z}/p)^*$ is cyclic, so is R. Furthermore, $|R| = |N| = \frac{p-1}{2}$.

Lemma 2.4.

(1) *K is cyclic and consists of the maps $z \to az$, a in R.*
(2) *No element of G fixes more than 2 letters.*

Proof. $|G_\infty| = \frac{|G|}{p+1} = p\left(\frac{p-1}{2}\right)$. The Sylow theorems then show that the group of translations is the unique p-Sylow subgroup of G_∞, and so is normal in G_∞. So for τ in G_∞, $\tau \circ (z \to z+1) = (z \to z+a) \circ \tau$ for some a in $(\mathbb{Z}/p)^*$. If τ is in K, $\tau(0) = 0$. Since $\tau(z+1) = \tau z + a$, $\tau(z) = az$ for all z in $\mathbb{Z}/p$. Now the maps $z \to az$, a in $(\mathbb{Z}/p)^*$, form a cyclic group of order $p-1$. Since K is a subgroup of that group of order $\frac{p-1}{2}$ we get (1).

Suppose next that $\tau \neq e$ fixes 3 or more letters. By double transitivity we may assume that 2 of these letters are 0 and ∞, so that τ is in K. But the only map $z \to az$ fixing a third letter is e. $\square$

Lemma 2.5. *Suppose $\tau \in \bar{K}$.*

(1) *If $p \equiv 1\ (4)$, $-1 \in R$ and τ stabilizes R and N.*
(2) *If $p \equiv 3\ (4)$, $-1 \in N$ and τ interchanges R and N.*

Proof. By Lemma 2.4 (1), the orbits of K acting on $(\mathbb{Z}/p)^*$ are R and N. Since τ normalizes K it permutes these orbits. Suppose first that $p \equiv 1\ (4)$. Then $|R| = \frac{p-1}{2}$ is even and R contains an element of $(\mathbb{Z}/p)^*$ of order 2, which must be -1. Furthermore by Lemma 2.4 (1), $z \to -z$ is in G and has an orbit (u, v) of size 2. By double transitivity some conjugate, λ, of this element lies

in $\bar{K}$, and, like $z \to -z$, fixes 2 letters. Such a λ cannot possibly interchange R and N. So it stabilizes R and N, and since $\bar{K}$ is a coset of K in H, the same is true of all τ in $\bar{K}$. Suppose next that $p \equiv 3\ (4)$. Then $|R| = \frac{p-1}{2}$ is odd, so -1 cannot be in R. If the lemma fails there is a τ in $\bar{K}$ with $\tau(1)$ in R. Since $\bar{K}$ is a coset of K in H there is a λ in $\bar{K}$ with $\lambda(1) = 1$. Then $\lambda \circ \lambda$ fixes the letters 0, ∞ and 1. By Lemma 2.4 (2), λ has order 2 and fixes 1. Since λ is a product of disjoint 2-cycles, λ must fix a second letter as well. By double transitivity some conjugate of λ is an order 2 element of K. But $|K| = \frac{p-1}{2}$ is odd. $\square$

Lemma 2.6. Suppose $\tau \in \bar{K}$. Then there is an n such that whenever z is in $(\mathbb{Z}/p)^*$ and a is in R, $\tau(az) = a^n \tau(z)$. Furthermore $\frac{p-1}{2}$ divides $n^2 - 1$.

Proof. τ normalizes K. So $\sigma \to \tau\sigma\tau^{-1}$ is an automorphism of K which is of the form $\sigma \to \sigma^n$ since K is cyclic. Then $\tau \circ (z \to az) = (z \to a^n z) \circ \tau$, giving the first result. Since the square of the automorphism is the identity, $\frac{p-1}{2}$ divides $n^2 - 1$. $\square$

Remark. n is prime to $\frac{p-1}{2}$. So when $p \equiv 1\ (4)$, n is odd. We're free to modify n by $\frac{p-1}{2}$, and so when $p \equiv 3\ (4)$ we may (and shall) assume that n is odd as well.

3 The case $p \equiv 1\ (4)$

In this section $p \equiv 1\ (4)$. Our first goal is to show that the n of Lemma 2.6 can be chosen to be -1.

Definition 3.1. X is the set of pairs whose first element is a τ in G, and whose second element is a size 2 orbit $\{u, v\}$ of τ.

Lemma 3.2. $|X| = \left(\frac{p^2+p}{2}\right)\left(\frac{p-1}{2}\right)$.

Proof. The number of size 2 subsets of $\mathbb{Z}/p \cup \{\infty\}$ is $\frac{p^2+p}{2}$. We prove the lemma by showing that for each such subset $\{u, v\}$ there are exactly $\frac{p-1}{2}$ elements of G having $\{u, v\}$ as an orbit. By double transitivity we may assume $\{u, v\} = \{0, \infty\}$. But τ has $\{0, \infty\}$ as an orbit precisely when τ is in $\bar{K}$. $\square$

Lemma 3.3. Every element of $\bar{K}$ has order 2.

Proof. Since -1 is in R, $\tau : z \to -z$ is in K. The letters fixed by τ are 0 and ∞; it follows that every element of G commuting with τ stabilizes the set $\{0, \infty\}$ and lies in H. So the centralizer of τ in G has order at most

$|H| = p-1$, and the number of conjugates of τ is at least $\frac{|G|}{p-1} = \frac{p^2+p}{2}$. Call these conjugates τ_i. Like τ, each τ_i has $\frac{p-1}{2}$ orbits of size 2. So the number of pairs whose first element is some τ_i and whose second is an orbit of that τ_i is at least $\left(\frac{p^2+p}{2}\right) \cdot \left(\frac{p-1}{2}\right)$. By Lemma 3.2 these pairs exhaust X. Suppose now that λ is in $\bar{K}$. Then λ has a size 2 orbit, $\{0, \infty\}$, and so must be some τ_i, proving the lemma. □

Corollary 3.4. The n of Lemma 2.6 can be taken to be -1.

Proof. Take τ in $\bar{K}$, σ in K. By Lemma 3.3, $(\tau\sigma)(\tau\sigma) = e$ and $\tau = \tau^{-1}$. So $\tau\sigma\tau^{-1} = \sigma^{-1}$. Examining the proof of Lemma 2.6 we get the result. □

Corollary 3.5. There is a λ in $\bar{K}$ and a c in $(\mathbb{Z}/p)^*$ such that:

(1) $\lambda(z) = z^{-1}$ for z in R.
(2) $\lambda(z) = cz^{-1}$ for z in N.

Proof. By Lemma 2.5 there is a $\bar{K}$ in R with $\lambda(1) = 1$. The result now follows from Corollary 3.4 and Lemma 2.6 □

Suppose we can show that the c of Corollary 3.5 is 1. Then, composing λ with the element $z \to -z$ of K we deduce that $z \to -\frac{1}{z}$ is in G. So to prove the classification theorem for $p \equiv 1 \ (4)$ it's enough to show that $c = 1$.

Proposition 3.6. When $p \equiv 1 \ (4)$, $z \to -\frac{1}{z}$ is in G.

Proof. Let $\alpha(z) = 1 - \lambda(z)$ with λ as in Corollary 3.5. Since -1 is in R, α is in G. Using the fact that $\lambda \circ \lambda = e$ we see that $\alpha^{-1}(z) = \lambda(1-z)$. Now $\alpha(0) = \infty$, $\alpha(\infty) = 1$, $\alpha(1) = 1-1 = 0$. So $\alpha \circ \alpha \circ \alpha$ fixes the letters 0, ∞ and 1. By Lemma 2.4 (2), α has order 3.

Since $p \equiv 1 \ (4)$, $p-1$ is in R. As not all of $1, 2, \ldots, p-2$ are in R there is an x in R with $x-1$ in N. The paragraph above shows that $\alpha(\alpha(x)) = \alpha^{-1}(x) = \lambda(1-x)$. We'll use this to show that $c = 1$. Since $\lambda(x) = -\frac{1}{x}$, $\alpha(x) = \frac{x-1}{x}$ is in N. Consequently, $\lambda(\alpha(x)) = \frac{cx}{x-1}$. Then $\alpha(\alpha(x)) = \frac{x-1-cx}{x-1}$ while $\lambda(1-x) = -\frac{c}{x-1}$. So $x - 1 = cx - c$, and $c = 1$. □

4 $p \equiv 3 \ (4)$. The main case

In this section $p \equiv 3 \ (4)$.

Lemma 4.1. There is a unique λ in $\bar{K}$ with $-\lambda(1)\lambda(-1) = 1$. Furthermore λ has order 2.

Proof. Fix τ in $\bar{K}$. By Lemma 2.5, -1 and $\tau(1)$ are in N while $\tau(-1)$ is in R. So $u = -\tau(1)\tau(-1)$ is in R. Replacing τ by $z \to v\tau(z)$ with v in R multiplies $-\tau(1)\tau(-1)$ by v^2. Since there is a unique v in R with $v^2 = u^{-1}$ we get the existence and uniqueness of λ. By Lemma 2.5 there are a and b in R with $\lambda(a) = -1$, $\lambda(-b) = 1$. Taking n as in Lemma 2.6 we find that $a^n\lambda(1) = -1$, $b^n\lambda(-1) = 1$. Multiplying we see that $(ab)^n = 1$, so $ab = 1$. Now $-\lambda^{-1}(-1)\lambda^{-1}(1) = (-a)(-b) = 1$, and the uniqueness of λ tells us that $\lambda = \lambda^{-1}$. $\square$

Corollary 4.2. Choose n odd as in Lemma 2.6. Then there is a λ of order 2 in $\bar{K}$ and a c in N with

(1) $\lambda(z) = cz^n \qquad z$ in R
(2) $\lambda(z) = c^{-1}z^n \qquad z$ in N
(3) $c^n = c$

Proof. Take λ as in Lemma 4.1 and set $c = \lambda(1)$. By Lemma 2.5, c is in N. Since $\lambda(1) = c$, $\lambda(-1) = -\frac{1}{c} = \frac{1}{c} \cdot (-1)^n$. Lemma 2.6 then gives (1) and (2). Since c is in N, $\lambda(c) = c^{-1} \cdot c^n$. But as λ has order 2, $\lambda(c) = 1$. $\square$

Lemma 4.3. Let $\alpha(z) = 1 - c^{-1}\lambda(z)$ with c and λ as above. Then α is an element of G of order 3 and $\alpha^{-1}(z) = \lambda(c(1-z))$.

Proof. Since c is in N, $-c^{-1}$ is in R, and α is in G. Also $\alpha(0) = \infty$, $\alpha(\infty) = 1$ and $\alpha(1) = 1 - c^{-1} \cdot c = 0$. So $\alpha \circ \alpha \circ \alpha$ fixes the letters 0, ∞ and 1; by Lemma 2.4 (2), α has order 3. Finally if μ is the map $z \to \lambda(c(1-z))$, then $\mu(\alpha(z)) = \lambda(\lambda(z)) = z$, and so $\alpha^{-1} = \mu$. $\square$

The proof of the classification theorem for $p \equiv 3 \ (4)$ now divides into 2 subcases. In this section we treat the "main case" where the c of Corollary 4.2 is -1, showing that $n \equiv -1 \ (p-1)$ so that $\lambda(z) = -\frac{1}{z}$ for all z. The "special case", $c \neq -1$, which leads to conclusion (b) of the classification theorem will be handled in the next section — it's a bit more technical.

Lemma 4.4. In the main case the only solutions of $x^n = x$ in $(\mathbb{Z}/p)^*$ are 1 and -1.

Proof. Since $c = -1$, $c^{-1} = -1$, and $\lambda(x) = -x^n$ for all x in $(\mathbb{Z}/p)^*$. Thus $\alpha(x) = 1 - x^n$. Suppose now that $x \neq 1$ is in $(\mathbb{Z}/p)^*$ with $x^n = x$. Then $\alpha(x) = 1 - x$ and so $\alpha(\alpha(x)) = 1 - (1-x)^n$. By Lemma 4.3, $\alpha^{-1}(x) = \lambda(x-1) = -(x-1)^n = (1-x)^n$. Since $\alpha(\alpha(x)) = \alpha^{-1}(x)$, $(1-x)^n = \frac{1}{2}$.

Raising to the nth power we find that $1-x=2^{-n}$. So 1 and $1-2^{-n}$ are the only possible solutions of $x^n=x$ in $(\mathbb{Z}/p)^*$. Since 1 and -1 are solutions we're done. $\square$

Proposition 4.5. Suppose $p \equiv 3\ (4)$. In the main case, λ is the map $z \to -\frac{1}{z}$, and so $z \to -\frac{1}{z}$ is in G.

Proof. By Lemma 4.4 the only solution of $x^n=x$ in the cyclic group R of order $\frac{p-1}{2}$ is 1. So $n-1$ is prime to $\frac{p-1}{2}$. Now $\frac{p-1}{2}$ divides $(n+1)(n-1)$ by Lemma 2.6. So it divides $n+1$, and as n is odd, $n \equiv -1\ (p-1)$. Then for z in $(\mathbb{Z}/p)^*$, $\lambda(z)=-z^n=-\frac{1}{z}$. Furthermore $\lambda(0)=\infty$, $\lambda(\infty)=0$. $\square$

5 $p \equiv 3\ (4)$. The special case

We continue with the notation of Section 4 but now assume $c \neq -1$

Lemma 5.1. Let x be a power of $-c$, and suppose that $1-x$ is in N. Then:

(a) $\alpha(\alpha(x)) = 1-c^{-2}(1-x)^n$
(b) $\alpha(\alpha(x^{-1})) = 1+x^{-1}(1-x)^n$
(c) $\alpha^{-1}(x) = c^2(1-x)^n$
(d) $\alpha^{-1}(x^{-1}) = -x^{-1}(1-x)^n$

Proof. Since $c^n=c$ and n is odd, $x^n=x$. Since c is in N, x is in R. Thus $\alpha(x)=1-c^{-1}(cx^n)=1-x$, and similarly $\alpha(x^{-1})=1-x^{-1}=\frac{1-x}{-x}$, which is in R.

Now $\alpha(\alpha(x))=\alpha(1-x)=1-c^{-1}c^{-1}(1-x)^n$ giving (a). And $\alpha(\alpha(x^{-1}))=\alpha\left(\frac{1-x}{-x}\right)=1-\left(\frac{1-x}{-x}\right)^n=1+x^{-1}(1-x)^n$ giving (b). Furthermore $\alpha^{-1}(x)=\lambda(c(1-x))$. Since $c(1-x)$ is in R, this is $c\cdot c(1-x)^n$. Finally $\alpha^{-1}(x^{-1})=\lambda\left(\frac{c(1-x)}{-x}\right)=c^{-1}\left(\frac{c}{-x}\right)\cdot(1-x)^n=-x^{-1}(1-x)^n$. $\square$

Lemma 5.2. In the situation of Lemma 5.1, $c^2+c^{-2}+2x^{-1}=0$.

Proof. $\alpha(\alpha(x))=\alpha^{-1}(x)$ by Lemma 4.3. (a) and (c) above tell us that $(c^2+c^{-2})(1-x)^n=1$. Similarly, (b) and (d) tell us that $2x^{-1}(1-x)^n=-1$. Adding these identities and noting that $(1-x)^n \neq 0$ we get the result. $\square$

Lemma 5.3. $c^3=-1$, and either $c^4+3=0$ or $3c^4+1=0$.

Proof. There is an x in $\{c^2, c^{-2}\}$ such that $1-x$ is in N. For neither $1-c^2$ nor $1-c^{-2}$ is 0, and if both were in R, their quotient, $-c^2$, would be in R.

Similarly there is a y in $\{-c, -c^{-1}\}$ such that $1 - y$ is in N. By Lemma 5.2, $c^2 + c^{-2} + 2x^{-1}$ and $c^2 + c^{-2} + 2y^{-1}$ are both 0. So $x = y$, and $c^3 = -1$. Also, since $c^2 + c^{-2} + 2x^{-1} = 0$, either $c^2 + 3c^{-2}$ or $3c^2 + c^{-2}$ is 0. $\square$

Proposition 5.4. $p = 7$. Furthermore either $c = 3$ and $\lambda = (0\infty)(13)(26)(45)$, or $c = 5$ and $\lambda = (0\infty)(15)(23)(46)$

Proof. Suppose $c^4 + 3 = 0$. Then, since $c^3 = -1$, $c = 3$. Also $27 = -1$ in $\mathbb{Z}/p$, and so $p = 7$. We know that $c^n = c$ in $(\mathbb{Z}/p)^*$. Since $c = 3$ is a generator of $(\mathbb{Z}/7)^*$, $z^n = z$ for all z in $(\mathbb{Z}/7)^*$. In particular if z is in R, $\lambda(z) = cz^n = 3z$, and so $\lambda = (0\infty)(13)(26)(45)$.

Suppose $3c^4 + 1 = 0$. Then since $c^3 = -1$, $3c = 1$. So $27c^3 = 1$, $-27 = 1$ in $\mathbb{Z}/p$, and once again $p = 7$. Since $3c = 1$, $c = 5$. Arguing as in the paragraph above we find that $\lambda = (0\infty)(15)(23)(46)$. $\square$

Suppose now that $c = 3$. Then $z \to z + 1$ is in G, and since 2 is in R, $z \to 2z$ is also in G. To complete the proof of the classification theorem for $c = 3$ it suffices to show that the group of permutations of $\mathbb{Z}/7 \cup \{\infty\}$ generated by $z \to z + 1$, $z \to 2z$ and λ is of order 168, and has a normal subgroup of order 8 (since G contains this group, and $|G| = 168$). This can be shown by brute force, but here's a conceptual argument using some of the theory of finite fields.

Let F be the field of 8 elements, ζ be a generator of F^*, and U be the group of permutations of F generated by $x \to x + 1$, $x \to \zeta x$ and $x \to x^2$. If r is in F^*, the conjugate of $x \to x + 1$ by $x \to rx$ is $x \to x + r$. It follows that $x \to x + 1$ and $x \to \zeta x$ generate the "affine group" of F, a group of order $7 \cdot 8 = 56$. Furthermore $x \to x^2$ is a permutation of F of order 3 normalizing the affine group. We conclude that $|U| = 56 \cdot 3 = 168$. The translations $x \to x + a$ evidently form a normal subgroup of U with 8 elements.

Now identify F with $\mathbb{Z}/7 \cup \{\infty\}$ by mapping 0 to ∞ and ζ^i to i. Then U may be viewed as a group of permutations of $\mathbb{Z}/7 \cup \{\infty\}$ of order 168. $x \to \zeta x$ is the permutation $z \to z + 1$, while $x \to x^2$ is the permutation $z \to 2z$. Now ζ has degree 3 over $\mathbb{Z}/2$, and so $\zeta^3 + \zeta + 1 = 0$ or $\zeta^3 + \zeta^2 + 1 = 0$. Choose ζ so that $\zeta^3 + \zeta + 1 = 0$. Then, $1 + 1 = 0$, $1 + \zeta = \zeta^3$, $1 + \zeta^2 = \zeta^6$ and $1 + \zeta^4 = \zeta^{12} = \zeta^5$. So $x \to x + 1$ is the permutation $(0\infty)(13)(26)(45)$ of $\mathbb{Z}/7 \cup \{\infty\}$. Thus the group generated by $z \to z + 1$, $z \to 2z$ and $(0\infty)(13)(26)(45)$ identifies with U, and has order 168, and a normal subgroup of order 8. The argument is the same when $c = 5$, except that we now take ζ with $\zeta^3 + \zeta^2 + 1 = 0$.

6 Simplicity results for $PSL_2(F)$ and final remarks

The simplicity result of Galois has been generalized in various ways. For example if F is any field with more than 3 elements, finite or infinite, then $PSL_2(F)$ is a simple group. I'll give one of the many proofs of this result. Let N be a normal subgroup of $SL_2(F)$ containing some non-scalar matrix. If suffices to show that $N = SL_2(F)$.

Lemma 6.1. There is an $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in N with $b \neq 0$.

Proof. If not, then since N is normal, every element of N also has $c = 0$, and so is diagonal. But if $\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$ is a non-scalar element of N, the conjugate of $\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ isn't diagonal. □

Now let P and P' be the subgroups $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ of $SL_2(F)$. P and P' evidently generate $SL_2(F)$. Since N is normal, $PN = NP$, and is the subgroup of $SL_2(F)$ generated by P and N.

Remark. If we can show that $N \supset P$, then since it is normal it also contains P', and so $N = SL_2(F)$.

Lemma 6.2. $PN = NP = SL_2(F)$.

Proof. Take $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in N as in Lemma 6.1. Multiplying this matrix on the left by $\left(\begin{smallmatrix} 1 & 0 \\ r & 1 \end{smallmatrix}\right)$ has the effect of adding $r\cdot$ (row 1) to row 2. So PN contains a matrix $\left(\begin{smallmatrix} a & b \\ * & 0 \end{smallmatrix}\right)$. Multiplying this new matrix on the right by $\left(\begin{smallmatrix} 1 & 0 \\ s & 1 \end{smallmatrix}\right)$ has the effect of adding $s\cdot$ (column 2) to column 1. So $PNP = PN$ contains a matrix $\left(\begin{smallmatrix} 0 & b \\ * & 0 \end{smallmatrix}\right)$. This matrix conjugates P into P'. So PN contains P' as well as P, and is all of $SL_2(F)$. □

Proposition 6.3. If $|F| > 3$, $N \supset P$. So by the remark above, $N = SL_2(F)$. Consequently $SL_2(F)$ is simple.

Proof. Take $a \neq 0$, 1 or -1 in F and let $d = a^{-1}$. By Lemma 6.2, $\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ -r & 1 \end{smallmatrix}\right) \cdot B$ for some B in the normal subgroup N. Then $B = \left(\begin{smallmatrix} 1 & 0 \\ r & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ ra & d \end{smallmatrix}\right)$. A short calculation shows that as A runs over all the elements of P, $(ABA^{-1}) \cdot B^{-1}$ also runs over all the elements of P. Since each $(ABA^{-1}) \cdot B^{-1}$ is in N, we're done. □

In presenting the material of this note to a class one might add the following remarks:

(1) Let F be the field of q elements where q is a prime power. Then $PSL_2(F)$ has order $\frac{q^3-q}{2}$ or q^3-q according as q is odd or even. By Proposition 6.3 these groups are simple for $q > 3$.

(2) If F is the field of q elements it's true that the "only" simple group having the same order as $PSL_2(F)$ is $PSL_2(F)$ itself. But I think that all proofs of this generalization of Frobenius' result are very difficult. The case $q = 4$ is trivial — since $4^3 - 4 = \frac{5^3-5}{2} = 60$, uniqueness when $q = 4$ follows from the uniqueness when $q = 5$. The next cases of interest are $q = 9$ when $|G| = \frac{9^3-9}{2} = 360$, and $q = 8$ when $|G| = 8^3 - 8 = 504$. In 1893, F. N. Cole, [3] (best known to mathematicians for the establishment in his honor of the Cole prize), used intricate arguments to handle these cases. He starts by showing that G is isomorphic to a doubly transitive permutation group on $q+1$ letters. But this is no longer an easy consequence of Sylow theory, as it is in the case of prime q.

(3) For $n > 2$, let $SL_n(F)$ be the group of n by n determinant 1 matrices with entries in F, and $PSL_n(F)$ be the quotient of $SL_n(F)$ by the group of determinant 1 scalar matrices. It can be shown that for all F and for all $n > 2$ the group $PSL_n(F)$ is simple. But now the generalization of Frobenius' theorem has an exception. If F is the field of 4 elements then $PSL_3(F)$ and $PSL_4(\mathbb{Z}/2)$ are non-isomorphic simple groups of order 20,160. (The group of even permutations of 8 letters is also simple of order 20,160, but it is isomorphic to $PSL_4(\mathbb{Z}/2)$.)

References

[1] F. G. Frobenius. Über Gruppen des Grades p oder $p+1$. Gesammelte Abhandlungen v. 3, 223–229.

[2] E. Galois. Oeuvres Mathématiques (deuxième édition, 1951), pages 57–59 and page 28.

[3] F. N. Cole. Simple Groups as far as order 660. Amer. J. of Math., v. 15 no. 4 (1893), 303–315.